November 2023

Key messages on the EC evaluation of the GDPR

The insurance industry welcomes the opportunity to provide input to the European Commission for the next evaluation of the General Data Protection Regulation (GDPR) foreseen in 2024. As data processing lies at the very heart of insurers' business, they are aware of the value of data and the importance of protecting it. Now that the GDPR has been in force for over five years, it has become apparent that work is needed to address problems in some specific areas of the legislation to ensure that the GDPR meets its objectives, which are to safeguard Europeans' fundamental right to have their privacy and personal data protected and to drive businesses to compete responsibly in the digital world.

Like many other sectors, the insurance industry has invested significant resources in understanding the Regulation and its implications for the sector and to ensure proper implementation of the new regime. At a time when the GDPR has set itself as a global standard, the Commission should consider all possible options to address the text's shortcomings within the existing legislative framework or to use appropriate complementary measures before considering proposing any amendments to the GDPR.

In view of the above considerations, the upcoming evaluation report should assess:

- The impact of the GDPR on **innovation** and address any obstacles the Regulation may have unintentionally created to the development of innovative and emerging technologies such as blockchain, artificial intelligence, big data or the internet of things. These technologies offer great opportunities for insurers and consumers, but innovation in the sector could be undermined if it challenges GDPR provisions and/or EDPB guidelines.
- The tools for **international data transfer** to third countries and suggest ways to address any existing insufficiencies to ensure that European companies can rely on the tools provided in the GDPR and that complying with them is not overly burdensome for firms.
- The **role of the European Data Protection Board (EDPB)** and the impact of its GDPR guidelines on the EU industry. Guidelines can be useful implementation and compliance tools. However, there are areas, such as international data transfers, right of data access and data breaches, in which the EDPB has not consistently applied the risk-based approach and proportionality principles enshrined in the GDPR as a result of a political agreement at EU level. The EDPB should increase its efforts in terms of transparency and communication. An increased dialogue with stakeholders would enable the EDPB to learn more about emerging issues and develop relevant guidelines that better align with the practical realities faced by businesses, ultimately promoting more robust and effective data protection compliance.
- The need to identify the right **legal basis at EU level** for the processing of health data for the conclusion and performance of insurance contracts. In order to ensure legal certainty and address barriers to cross-border data transfers, it should be clarified that the processing of health data necessary for this purpose is covered by one of the derogations in the GDPR, such as the one in Art. 9 (2) (f).

Each topic is further elaborated in the sections below.

1 International data transfers

- Insurance Europe welcomes the adoption of the new **EU-US Data Privacy Framework** and calls on the EC to continue its work to develop new adequacy decisions that allow for the lawful transfer of data outside of the EU while respecting the privacy of EU citizens. Adequacy decisions are the most well-fitting instrument for insurers to transfer data internationally as they provide the

most appropriate safeguards for both data controllers and data subjects. However, the current list of countries that are covered by an adequacy decision is still quite limited and falls short of covering data transfers in an environment in which the global exchange of data is on the rise daily. The EC should take note of this gap and speed up the processes for adopting adequacy decisions for third countries and territories with an adequate level of protection.

- With the spectre of a possible "*Schrems III*" case around the corner, the insurance industry calls for continued legal certainty so that EU companies can continue to carry out their business activities. EU companies are still facing severe challenges assessing the legal requirements of third countries. With the use of standard contractual clauses (SCCs) and binding corporate rules now dependent on companies' ability to ensure that privacy standards in the receiving jurisdiction are adequate, companies must now rely on their own resources to conduct **burdensome assessments**. Rather than investing in a multitude of global law firms providing expertise in each jurisdiction, it should be for the Commission to determine whether the local laws and customs of a third country represent an obstacle to the transfer of personal data to that country.

- In its Recommendations 1/2020, the EDPB calls for additional safeguards when using third-country transfer instruments, eg, SCCs. In practice, it is often not possible to take the protective measures required by the data protection authorities. Unfortunately, the authorities do not apply the **risk-based approach** inherent in the GDPR in this respect. This often makes cloud solutions impossible to use even in the case of very low risk, such as a business video conference with the use of exclusively professional contact data. Art. 24 and 32 GDPR provide for a risk-based approach to the determination of technical and organisational measures for the protection of data subjects. Although this risk-based approach is not explicitly stated in the regulations on transfers to third countries in the GDPR (Art. 44 ff), it should also apply here without restriction.

- The GDPR already provides alternative tools for international transfers. The derogations provided for in Art. 49 GDPR for cases in which the level of data protection in third countries is not adequate could be helpful but they **should not be interpreted too narrowly**. For example, Art. 49 (1) (a) GDPR permits data transfers on the basis of the data subject's explicit consent after being informed of the possible risks of such transfers. The exceptional nature of the provision is already accounted for through the increased informational requirements compared with consent pursuant to Art. 6 and 9 GDPR. In contrast, there are no restrictions on the possibility of consent either in the wording or in the recitals. The EDPB should therefore be notified that the requirement to only allow consent in exceptional cases imposes a new restriction that was not originally envisaged by co-legislators at the time the GDPR was finalised.

- The current very low number of **code of conducts** can be linked to the high requirements imposed by the EDPB. In its Guidelines 1/2019, the EDPB stated that the establishment of a private monitoring body is an indispensable condition for approving any code of conduct. However, according to Article 41 GDPR, which is designed as a "may" clause, the establishment of a private monitoring body is optional. Due to the fact that the GDPR must apply to all industries, codes of conduct, which include industry-related specifications, create legal certainty for users and facilitate the work of the supervisory authorities. Article 40(1) GDPR therefore rightly specifies the legislators' objective to encourage the drawing up of codes of conduct. There are concerns, however, that the high requirements of the EDPB might impede the achievement of this objective. Therefore, consideration should be given to initiatives aimed at ensuring that monitoring bodies are considered optional.

- The Recommendations 1/2022 of the EDPB on **Controller Binding Corporate Rules** (BCRs) and the very long duration of the approval process in practice so far make BCRs within the meaning of Art. 47 GDPR as an instrument for data transfers to third countries increasingly unattractive for corporate groups. According to the Recommendations, the BCR regulations must now map practically the entire requirements of the GDPR. In addition, the BCRs must provide for a large number of additional measures that go beyond Art. 47 of the GDPR. The EDPB has thus significantly expanded the requirements for BCRs in the working papers WP 256 and WP 264 of the Art. 29 Working Party after only a short period of validity and — with the exception of the Schrems II case law — without any discernible external reason. Against this background, the labour-intensive preparation of new BCRs or the adaptation of existing BCRs and their implementation, which involve a great deal of effort for all group members, is hardly worthwhile any more.

In brief

- The Commission should speed up the processes for adopting adequacy decisions for third countries and territories with adequate levels of protection. Efforts should be made to maintain the EU-US Data Privacy Framework and the EU-UK adequacy.

- The Commission and the EDPB should explore further practical solutions to ease the burden caused by the *Schrems II* judgment on companies.
- The Commission should take measures to ensure that companies can make full use of all the tools for international transfers provided in the GDPR. At this stage, the use of codes of conduct and BCRs has been limited due to the high requirements imposed by the EDPB and long and complex approval processes. Derogations provided for in Art. 49 GDPR should also not be interpreted too narrowly.

2 Barriers to new technologies

- So far, there is no clear legal basis for the **training and testing of new IT applications and systems**, especially with special categories of personal data (eg, health data). The Commission's proposal for a Regulation establishing harmonised rules for artificial intelligence (AI Regulation) does provide a legal basis in Art. 10(5). However, this is unfortunately limited to the development of high-risk AI and only applies insofar as this is absolutely necessary for the purposes of preventing discrimination. Since it is in the public interest that AI and other IT systems arrive at correct results, tests with pseudonymised real data, including health data, should be explicitly permitted.

- The underlying principles of blockchain technology raise certain questions about compatibility with the GDPR. For example, how to reconcile the GDPR's rights to erasure and to rectification with the fact that blockchain technology is designed to be an immutable and permanent record of all transactions is unclear. This lack of clarity may hinder the development of solutions based on blockchain technology by insurers. The EC should take note that the principle of "technological neutrality" should be preserved in any legislation and guidance. Insurance Europe recommends that the EC works closely with the EDPB to address any necessary clarifications of the interplay between the GDPR and blockchain and to provide the necessary legal certainty to develop solutions based on blockchain technology.

- The interpretation of Art. 6 (1) (b) GDPR in the Guidelines 2/2019 hampers digitalisation because its understanding of what is "**necessary**" for the performance of a contract is too restrictive. The interpretation of Art. 22 (2) (a) GDPR in WP 251 of the Article 29 Data Protection Working Party, which was endorsed by the EDPB on 25 May 2018 icorresponds. Data protection authorities are of the opinion that automated decision-making is not necessary for the performance of a contract because until now human beings performed this task. They draw the conclusion that automated decision-making is not permissible and that an effective consent according to Art. 22 (2) (c) Art. 7 (4) GDPR can only be given if the data subject has the opportunity to choose processing by a human being from the beginning. However, such a narrow interpretation of need would prevent insurers and consumers from fully accessing the benefits of new technology. For example, an insurance company may offer online motor insurance through a mobile phone app where the consumer can obtain coverage simply by sending a picture of the car and providing the requested data via an app. In this case, the premium is automatically calculated and the contract is entered into when the payment is effective. This is an example of solely automated decision-making that falls under Article 22 (2) (a). As a safeguard, the data subject has the right to obtain human intervention and ultimately to contest the decision pursuant to Article 22 (3). If the data of third parties is processed, eg, in third-party liability insurance, the exemption in Art. 22 (2) (a) GDPR is not applicable. Obtaining the consent of the third party is often not possible or at least not easy. To ensure that Art. 22 does not become an obstacle to digitalisation, it should be made clear that it is **a right of the data subject and not a prohibition**. This ensures that claims by customers and injured parties in the insurance industry can be checked quickly and unbureaucratically. Anyone who is dissatisfied with a decision is sufficiently protected by the possibility to challenge it.

- Digitalisation requires more analysis of data, for which anonymised data is often sufficient. However, if — as suggested in recital 26 — personal data is defined in absolute terms and not in relation to the respective data controller, it is difficult to justify that data is ever **truly anonymised**. Here, the GDPR should take a clear relative approach, as adopted by the General Court, judgment of 26.4.2023, T-557/20). The requirements of data protection authorities for data controllers to continuously ensure that their procedures are still sufficient to adequately limit the remaining risks of reidentification and to adapt their measures if necessary is practically impossible to fulfil with increasing data-sharing.

In brief

- The Commission or the EDPB should provide the necessary clarifications to ensure that:
  - What is considered "necessary" for the performance of a contract is not considered too restrictive to ensure that Art. 22 does not become an obstacle to digitalisation.
  - There is a clear legal basis for the training and testing of new IT applications and systems, especially with special categories of personal data (eg, health data).
- There is a need for further guidance on:
  - The interplay between the GDPR and blockchain technologies
  - The technical methods that can be used to render data anonymous in compliance with the GDPR

3 Role of the EDPB

- The EC, as the guardian of European law, should include a dedicated section in the report on the role of the EDPB and the impact of its GDPR guidelines and recommendations on industries. In particular, this section should address the areas in which the interpretation of the EDPB has gone beyond the political agreement in the text of the GDPR by, for example, creating additional requirements or narrowing the interpretation of GDPR provisions (see annex). The EC should use the report on the application of the GDPR to reinforce its role as the guardian of the Regulation and to stress that the EDPB's mandate is subject to the political agreement in the text of the GDPR. The EDPB should also increase its efforts in terms of transparency, engagement and communication. An increased dialogue with external stakeholders would enable the EDPB to learn more about emerging issues and develop relevant guidelines that better align with the practical realities faced by businesses, ultimately promoting more robust and effective data-protection compliance.

In brief

- The EDPB should have a more structured dialogue with external stakeholders to ensure that future guidelines better reflect the reality and needs of businesses and civil society. Stakeholders should be involved at an earlier stage in the preparation of the guidelines.

- A key example of where the EDPB guidelines have gone beyond the political agreement in the text of the GDPR are the guidelines on the **right of access**. The EDPB interpretation will result in a more burdensome handling of data-access requests without any clear benefits for the data subjects.
  - For example, the guidelines suggest that the controller should provide access as requested by the data subject, including to personal data stored in the back-up. Requiring the controller to search back-up systems, which may not be readily or easily accessible, constitutes a disproportionate effort. Back-up data is personal data stored solely for the purpose of restoring the data in the case of a data-loss event and therefore should not be included in the scope of the right of access.
  - The guidelines state that Art. 12 (5) on manifestly unfounded requests should be interpreted narrowly and that an access request should not be regarded as excessive unless the data subject clearly declares that the request is malicious in its intent. This seems to disregard and contradict national procedural law in many member states. Whether a request for access is excessive cannot be made dependent on whether the data subject expressly makes its abusive intentions known. Furthermore, data holders should be able to **refuse access requests** if it is apparent that the data subject only pursues **goals unrelated to data protection**. As set out in Recital 63, this right should not adversely affect the rights or freedoms of others, including **trade secrets or intellectual property**.
  - Finally, tailoring the processed information to each access request would be materially impossible for controllers, who may regularly receive a large number of requests. In order to offer transparent and effective information, as well as to limit the impact on the controller's operations, it would be advisable if the controller could implement a layered

approach. Controllers could, as a first step, provide access to the information required by Article 15 (1) (a) – (h) and (2) in a general manner — similarly to a privacy notice — and then ask the data subject whether more tailored information needs to be provided. Based on members' experience, the majority of data subjects just want access to their data and are uninterested in Art. 13/14 detail specific to them. Therefore, unless the data subject explicitly requests such tailored information after being asked for specification, a general overview of processing activities should be able to fulfil the controller's obligation.

- Other examples include:
  - The EDPB guidelines on the interplay between **Art. 3 and Chapter V GDPR** have been useful as they provide clarity on the key criteria to qualify a processing as a transfer of personal data to a third country. However, the qualification as a data transfer to a third country should not only depend on the parties involved in the processing, but should also factor in the data concerned. In particular, the EDPB should clarify that processors established in the EU/EEA do not have to comply with the provisions on transfers of personal data to third countries under the GDPR when transferring back data originated by a non-EU controller. Indeed, if the processor merely processes and transfers back personal data that has been received from the third-country controller without combining that data with personal data collected by the processor itself, the processor does not disclose any "new" data to a "new" recipient. The processor merely returns the data to the country that is its place of origin. Therefore, no increased risk arises from the transfer of the data back to the "third country". In these cases, the requirement to use Article 46 safeguards for the transfer back would expand obligations resulting from the GDPR to data processing that does not even fall under the GDPR's territorial scope of application in the first place.
  - As mentioned above, the Recommendations 1/2022 of the EDPB on **Controller BCRs** and the very long duration of the approval process in practice make BCRs within the meaning of Art. 47 GDPR as an instrument for data transfers to third countries increasingly unattractive for corporate groups.

4 Legal basis for health data processing

- In order to lawfully process special category data, an insurer needs to identify both a lawful basis under Article 6 of the GDPR and a separate condition for processing under Article 9.

- Article 9 (4) GDPR specifies that member states may "maintain or introduce additional conditions, including limitations, with respect to the processing of genetic data, biometric data or data concerning health". This provision creates legal uncertainty for insurance bodies in member states that have not made specific provision for health data processing in the field of insurance. In the absence of a specific national provision, insurers can only process health data based on **consent**. However, using consent as a legal ground for the processing of health-related data has many disadvantages:
  - Gathering explicit consent for insureds, policyholders and beneficiaries can be burdensome.
  - Reinsurers do not always have a direct contractual relationship with the data subjects whose health-related data is being processed, making it difficult to obtain their consent.
  - Once obtained, consent can be withdrawn at any time; consent is hence not a sufficiently reliable and efficient legal ground for the performance of an insurance contract.

- The validity of the consent could be challenged as the conclusion and performance of an insurance contract is often simply not possible without the processing of health-related data. It could be argued that the consent was not freely given since the performance of the contract is dependent on the insured's consent. Such processing can only be carried out with the application of the exception in Art. 7.4 of the GDPR[1]. However, the EDPB in its Guidelines 5/2020 on consent states that: "Since the wording of Article 7(4) is not absolute, there could be a very limited number of cases where this conditionality would not render consent invalid".

1 Article 7(4) says that "when assessing whether consent is freely given, utmost account shall be taken of the fact that whether, among others, the performance of a contract, including the provision of a service, is made conditional on the consent to the processing of data that is not necessary for the performance of the contract"

- Due to the different conditions used in member states for the processing of health data for an insurance contract, there are also obstacles to cross-border data transfers within the EU. There is therefore a need for a clarification at EU level of the right legal basis for the **processing of health data for the conclusion and performance of insurance contracts**. The Commission or the EDPB should clarify that the processing of health data necessary for the performance of insurance contracts and for claims settlement (including reinsurance) can be covered by another derogation in the GDPR, such as the one provided in Art. 9 (2) (f) GDPR.

In brief

- In order to ensure legal certainty and address barriers to cross-border data transfers, the Commission or the EDPB should clarify that the processing of health data necessary for the performance of insurance contracts and for claims settlement (including reinsurance) can be covered by another derogation such as the one in Art. 9 (2) (f) GDPR.